

Appendix C

EMS Communications and Encryption

TABLE OF CONTENTS

Section	Description	Page
C.1	DIGITAL SERVICE	C-5
C.1.1	CISCO 7206 ROUTER	C-5
C.1.2	KENTROX D-SERV	C-6
C.1.3	KENTROX UNIVERSAL SHELF	C-6
C.1.4	DEDICATED LINES	C-6
C.1.5	COMMUNICATION SERVICES	C-6
C.1.6	IPsec AND CISCO ROUTER REQUIREMENTS	C-8
C.2	INTERNET SERVICE	C-9
C.3	TELNET OPTIONS	C-11
C.4	ZMODEM OPTIONS	C-11

This page intentionally left blank!

EMS COMMUNICATIONS AND ENCRYPTION

The Memphis and Martinsburg Computing Centers offer a variety of communications services and capabilities that allow TPs to file tax returns and electronic documents. These capabilities include both dedicated digital and Internet communication services as well as several file transfer protocols. The use of these features is summarized in this appendix.

As of November 1, 2005 analog and IRS ISDN services are no longer available. However, it may be possible for a TP to use ISDN if he/she provides his/her own equipment.

C.1 DIGITAL SERVICE

Use of digital services requires authorization from the IRS. Please contact Darryl Giles at (202) 283-5193, e-mail darryl.s.giles@irs.gov.

As of November 1, 2005, all dedicated lines must be encrypted using at least 128-bit encryption provided by a Federal Information Processing Standards (FIPS) approved method. A TP, using the digital service, is responsible for choosing, procuring, and installing his/her cryptographic solution. To determine if a cryptographic solution meets FIPS standards obtain the "NIST Validation List Certification Number and Date" from the solution provider. This information can be verified by checking the NIST website at <http://csrc.nist.gov/cryptval/>. There are validation lists for each major FIPS Cryptographic Standard. Each list has a sequence number, and lists the manufacturer/supplier, date of validation, name of the implementation, its operational environment, and a further description of other characteristics.

The IRS recommends the use of Internet Protocol Security (IPsec) as the cryptographic solution for the digital service. Additional information for TPs who use Cisco routers and may need to upgrade them to support IPsec is provided in Section C.1.6.

The following paragraphs describe the hardware and software necessary to use the digital communication service.

C.1.1 CISCO 7206 ROUTER

Two (2) Cisco 7206 routers have been installed in both Martinsburg and Memphis. Each Cisco 7206 has an aggregate bandwidth of 600 Mbps and contains six slots for communications adapters. While one of the routers is a hot spare, the active 7206 is configured as follows:

- One (1) Ethernet adapter with four (4) ports--10 Mbps each port
- One (1) High speed synchronous adapter, which supports eight (8) ports

- One (1) High speed synchronous adapter, which supports four (4) ports
- All high speed synchronous ports support speeds up to 2.048 Mbps. Connections to these ports are mostly through the Kentrox unit described next, although some TPs have connected to the interfaces, directly from their own high-speed communications equipment

TPs use either Point-to-Point Protocol (PPP) or Frame Relay link encapsulation when connecting to the high speed synchronous ports.

C.1.2 KENTROX D-SERV

The Kentrox D-SERV is the Channel Service Unit/Digital Service Unit (CSU/DSU) to be used by TPs desiring a direct connect 56 Kbps digital circuit. It meets all the requirements of the AT&T Technical Publications TR 62310 and TR 41450. TPs must purchase a D-SERV unit and a 56 Kbps digital circuit to begin testing over a dedicated line. The D-SERV unit ordered by the TP must be designed for connection to the Kentrox Universal Shelf listed below. The D-SERV interface cards should be configured as follows:

- V.35 interface--configuration switch S1 UP and interface switches S1-S5 DOWN and S6-S10 UP.
- Constant Carrier--configuration switch S2 DOWN.
- Data Clock--56 Kbps, synchronous, internal clock. S3 UP, S4 DOWN, S5 UP, S6 UP and S7 DOWN.

C.1.3 KENTROX UNIVERSAL SHELF

A Kentrox Universal Shelf has been installed in the Memphis and Martinsburg Computing Centers. Each shelf supports up to twelve 56 Kbps D-SERV interface cards.

C.1.4 DEDICATED LINES

For a TP to connect over a dedicated line he/she must purchase the circuit. Once the TP's request for digital service is approved, the IRS provides him/her with IP addressing and routing information.

C.1.5 COMMUNICATION SERVICES

Connection to the EMS system using the digital communications services provides the TP with a Transmission Control Protocol/Internet Protocol (TCP/IP) interface. To use this service the TP must have the following:

- A system that supports the TCP/IP protocols.

- The ability to make a Telnet connection from his/her system to an EMS host.
- If the TP plans to use File Transfer Protocol (FTP) for data transfer, his/her system must support an FTP server and have the ability to accept an FTP connection from the EMS. The TP must supply a user logon and password for the EMS system to use when connecting to his/her FTP server.
- A router capable of supporting PPP or Frame Relay over the digital circuit.

Once the TP establishes a connection using EMS digital services the following capabilities are available.

- Connecting over a TCP/IP link allows a TP to connect to any host available to him/her at the computing center.
- Fail over protection. EMS systems have a fail over capability and if there is a system failure a backup system becomes available. This system uses the same TCP/IP address as the primary system. This allows the TP to connect to the backup system without having to reconfigure the host address.
- Transfer of data using FTP. If a TP has a host system that supports FTP, he/she may use this as a protocol to send and receive files to the EMS system. For TPs using this transfer method the only configuration needed is to setup a user account for EMS to use and directories for EMS to use to "get" return files and "put" acknowledgment files. EMS transmits one file for each acknowledgment file available for processing. The file transfers are binary and the "#" hash mark is displayed for every 1,024 bytes of data transferred.
- File transfers over Telnet. If a TP uses TCP/IP to connect to the EMS system, his/her logon to the system is through Telnet. If the TP does not want to use FTP to transfer files, he/she may use another file transfer protocol such as Zmodem over the Telnet session. This capability is currently available in many of the Telnet application programs. The file transfer rate of Zmodem over a Telnet session is not as fast as FTP. See Sections C.3 and C.4 for more details.
- One final aspect of a TCP/IP connection to the EMS is that TCP/IP supports multiple simultaneous connections to the same host or multiple hosts. A TP may submit files over multiple concurrent sessions. However, only one session per host can retrieve acknowledgment files.

C.1.1.6 IPsec AND CISCO ROUTER REQUIREMENTS

To support IPsec encryption, TPs with existing Cisco routers may need to upgrade their router's IOS® and memory to the minimum requirements listed in Exhibit C-1 for their specific platform. TPs that are registered Cisco users can download the newer IOS version from Cisco's website (www.cisco.com).

IOS versions will vary per router. As a rule, the IRS will use the highest 12.2 GD (General Deployment) release at the time of implementation with the following feature sets: IP PLUS/IPSEC 3DES.

**Exhibit C-1 Minimum Cisco IOS Version
and Memory Requirements**

Cisco Router Series	IOS Version	Memory
Cisco 800 Series	c800-k9osy6-mw.12.2-13.T (12/8) - IPsec Triple DES Encryption (IP/FW PLUS IPSEC 3DES)	DRAM - 12 MB Flash - 8 MB
Cisco 1700 Series	c1700-k9o3sy7-mz.12.2-13.T (48/16) - IPsec Triple DES Encryption (IP/FW PLUS IPSEC 3DES)	DRAM - 48 MB Flash - 16 MB
Cisco 2600 Series: (2602, 2610, 2611, 2620)	c2600-ik9o3s-mz.12.2-13.t (96/32) - IPsec Triple DES Encryption (IP PLUS IPSEC 3DES)	DRAM - 96 MB Flash - 32 MB
Cisco 7206 Series: (IRS owned and maintained)	c7200-ik9o3s-mz.12.2-13.T (128/16) - IPsec Triple DES Encryption (IP/FW/IDS IPSEC 3DES)	DRAM - 128 MB Flash - 16 MB

Depending on other functions used by the router (e.g., NAT, IOS firewall, several T1 lines, number of users), the CPU utilization can be seriously degraded by adding encryption functionality. It is recommended that acceleration modules be added. If possible, it is also recommended that the base router component be upgraded (i.e., 1700 to a 1750, 2600 to a 2650, etc.). There are no hardware upgrades or module additions for the 800 series routers; therefore, TPs using these routers should consider upgrading to a 1750 series router. The Cisco 1600 series and 2500 series routers do not support IPsec and must be upgraded. Cisco recommends an upgrade to the next highest platform. (i.e., 1600 Router to 1700 Router or 2500 Router to 2600 Router). See the Cisco website for details.

Those TPs that wish to purchase new routers can do so by purchasing Cisco's "VPN bundles." Exhibit C-2 identifies IRS recommended bundles.

Exhibit C-2 IRS Recommended Cisco VPN Router Bundles

Product Number	Description
CISCO1751-VPN/K9	1751 VPN Bundle with VPN Module, 64 MB DRAM, IP Plus/FW/3DES
CISCO1760-VPN/K9	1760 VPN Bundle with VPN Module, 64 MB DRAM, IP Plus/FW/3DES
CISCO1760-V3PN/K9	1760 VPN Bundle with VPN Module, 96 MB DRAM, IP Plus/VOX/FW/3DES
C2651XM-2FE/VPN/K9	2651XM/VPN Bundle, AIM-VPN/BPII/2FE/IOS FW/IPSec 3DES, 128DRAM
C2691-VPN/K9	2691 VPN Bundle, AIM-VPN/EPII, Plus FW/IPSEC 3DES, 128DRAM
C3725-VPN/K9	3725 VPN Bundle, AIM-VPN/EPII, Plus IOS FW/IPSEC 3DES, 128DRAM
C3745-VPN/K9	3745 VPN Bundle, AIM-VPN/HPII, Plus IOS FW/IPSEC 3DES, 128DRAM

C.2 INTERNET SERVICE

To use the Internet service, a TP accesses EMS via his/her own Internet Service Provider (ISP) and does not need to have a static IP address. However, the TP must use Telnet/SSL to provide a secure session. His/her Telnet/SSL software must conform to:

- RFC 854 - Telnet Protocol Specification
- SSL 3.0 Specification (<http://wp.netscape.com/eng/ssl3>)

The Telnet/SSL traffic must be transmitted to EMS on TCP port 992. The TP may need to configure his/her firewall(s) to allow this traffic to pass through. **This has been the most common cause of failure to connect to EMS through the Internet.** Most businesses routinely block traffic on ports not commonly used for security reasons. The TP connects to EMS using one of the following fully qualified Domain Name System (DNS) names.

- efileA.ems.irs.gov - Martinsburg Computing Center
- efileB.ems.irs.gov - Memphis Computing Center
- efileC.ems.irs.gov - Memphis Computing Center

ETA provides information on which processing sites are located at the two computing centers, and which DNS name above to use during the calendar year.

If the TP's software allows him/her to establish concurrent sessions to the same computing center, the TP may submit files over multiple concurrent sessions. However, only one session can retrieve acknowledgment files. TPs should note that FTP is not available as a file transfer protocol when using the Internet service.

Configuring Terminal Emulation Software

A TP may need to provide the following information when he/she is configuring their terminal emulation software.

- **Terminal Name.** Should be something meaningful to the TP. This information is not transmitted to EMS.
- **Terminal Type.** Select a member of the Virtual Terminal (VT) family (e.g., VT100 or VT220).
- **SSL Version.** SSL3. In many terminal emulation packages this is a pull-down menu beside the Destination or Host Name and is not labeled. TLS-1 defaults since it is the latest SSL version but SSL-3 must be chosen.
- **Port.** 992. This port number is often filled in automatically by the terminal emulation software if Telnet/SSL is chosen.
- **Destination or Host Name.** One of the fully qualified names listed previously.
- **Destination Host Type.** Unix.
- **User Certificate Mode.** No user certificate is required. However, EMS accepts any certificate from the TP. If the TP wants to send a certificate, it can be self-generated.
- **Host Certificate.** EMS sends an Entrust certificate, which the terminal emulation software must accept.
- **Certificate Viewing.** If the TP wants to see the certificates being exchanged and the terminal emulation software supports certificate viewing, then this feature should be turned on.
- **Operating System (OS).** If your terminal emulation software asks for an OS, it is asking about the Trading Partner's system, not the EMS system. Enter the local system parameters upon which the terminal emulation software will be running.
- **Data Characters.** Please specify eight bit data characters if your terminal emulation software does not default to it.

The IRS has tested several terminal emulation software packages supporting Telnet-SSL including PowerTerm Pro Enterprise for Unix Version 8.8.3, Hummingbird Exceed, and Attachmate. Many other commercial and open-source packages can also be used as long as they support the Telnet specification RFC 854 and the SSL 3.0 specification. If a TP cannot successfully connect using an internally developed package we recommend using one of the above packages, which can often be evaluated free, to verify the connectivity parameters outlined above. Additional guidance is given in C.3 and C.4.

C.3 TELNET OPTIONS

If the TP uses Zmodem, Xmodem-1K, or Ymodem-batch to transfer files over the Telnet session, to be successful the TP's Telnet program must support connections that allow all eight bits of the data to pass through. This is often accomplished on the Telnet command line as "telnet -8 host". If the TP uses the "telnet -8" method, the screen display may appear distorted and after typing in the TP identification information the systems appears to be hung. If this occurs the TP should terminate his/her responses with a Line-Feed Character. On a standard keyboard, depressing the Control Key and the "j" key at the same time generates this character. As an alternative to the "telnet -8" option, the TP may set binary mode before beginning a file transfer and unset binary mode upon completion of the transfer.

Most versions of Telnet have a sequence of characters (called an Escape Sequence) that, when encountered by the Telnet program, interrupts the Telnet session. Unless hidden by the TP's terminal emulation software, the TP normally sees a message displaying the Escape Sequence when the Telnet connection is first started. Although it is possible for the TP to have a successful session when an Escape Sequence exists, at some point a file transfer may abort based on its size or the data in the file. For this reason it is recommended that the Escape Sequence be disabled, if possible. The TP should check his/her Telnet documentation to determine how to do this.

C.4 ZMODEM OPTIONS

The most common file transfer software used over the Telnet Session is Zmodem. The package consists of the "sz" command for sending files and the "rz" command for receiving files. As with the Telnet session options described in Section C.3, there are options that may need to be invoked to achieve a successful file transfer. In addition, it is important to note that these options are not necessarily mutually exclusive from the Telnet options. It may be that having a specific Zmodem option set might mean that a Telnet option does not need to be invoked. It is recommended that TPs explore the Zmodem options first. These options are available if the TP is experiencing problems:

- **Zmodem Escape Control Characters.** This option, usually "-e", will have Zmodem watch for control characters and modify them so that they pass through undetected as control characters. The option is sometimes available on both the "sz" and "rz" commands. Other versions have the -e option available only on the "rz".
- **Zmodem Binary.** This is another option available on some versions of Zmodem. The TP should check his/her documentation for any option that attempts to make the link transparent to control character sequences.
- **Zmodem Timeout Values.** Within Zmodem there are options for how long to wait for an expected packet of data. The default is normally 10 seconds. In most cases, this

value should be acceptable. However, the TP should never set these values to wait forever.

- **Zmodem buffer timeout.** There may be times when the timeout values may need to be changed. This can occur with TPs, whose connection to their ISP is through a dial-up line. Because of the buffering ability of telecommunications equipment and the amount of communications equipment usually in place for an Internet connection, the amount of data that can be stored could cause an error. This can happen if a file that is to be transmitted is approximately the same size as one of the buffers present in the data link. The sending program will have completed the streaming of all the data in the file but the receiving side may not have gotten any data yet. If the sending side has its receive packet timeout set too low, it may timeout before the receiver can receive and transmit the packet.
- **Zmodem sliding window.** If this option is not enabled, the sender transmits all of a file without waiting for an acknowledgment. This results in a faster file transfer. However, some of the intermediate communications equipment may store data while it is transferred to the receiver. Sometimes this causes the sender to "get ahead" of the receiver. In this case, the TP may need to enable the sliding window option. This results in intermediate acknowledgments and a slower file transfer. The smaller the value of the sliding window setting the slower the file transfer.
- **Zmodem Debugging.** When testing the TP's Internet connectivity, the TP should become familiar with the debug capabilities of his/her Zmodem software. If the TP experiences problems with the transfer of data, generating a debug file could assist the TP and IRS system support personnel in determining the nature of the problem.
- **Crash Recovery.** EMS does not retain partial files. Therefore, if a transmission to EMS is interrupted, the TP must retransmit from the beginning of the file. For acknowledgment files and state return files, EMS can resume the transmission from where the interruption occurred in the transmission if the TP's software supports it.